

Check Windows' background tasks

Are your PC's resources being stretched by useless jobs or malware? Jon Thompson explains how to decipher hidden tasks

Windows PCs are usually busy, whether or not you are running a program such as a word processor, web browser or game. In the background, largely unseen, Windows manages a large collection of software that performs the often mundane tasks needed to support more apparently useful features such as extra-fast searching, internet access and USB device connections. These tasks are known as processes. Here we explain how to find out which are useful and which are wasting your PC's resources.

First, run the Task Manager by pressing Ctrl-Shift-Esc and click on the Processes tab. You'll see a confusing and long list of programs with no indication as to what each one does or what program is controlling them.

Processes form the running operating system and its applications. It is the job of the Windows kernel to manage them all. By finding out a little about how it does this, we can better understand what's going on and move on to learn about tools that will help manage and explore the system further.

Many strangely named processes are actually services: permanently running processes whose job it is to handle all the tasks Windows needs to undertake automatically, such as detecting new USB devices or checking for security updates. The kernel's management of those processes might be responsible for your computer becoming sluggish.

PAGING AND SWAPPING

Processes that occupy space in the system's RAM but do nothing are a drain on often-scarce memory resources. To speed things up, the kernel copies some of them to a part of the hard disk called the page file. It then re-uses the memory they occupied. This procedure is known as swapping.

If the kernel subsequently needs to use a swapped-out process, it will copy it back into RAM and continue running it. To make best use of all available RAM, the kernel will even swap out just the parts of a running process or its data that haven't been accessed for a while, and re-use the RAM they occupied. This is called paging. A page fault occurs when the kernel needs access to a piece of code or data in the page file, forcing it to load it back into RAM.

Together, the page file and RAM form the PC's virtual memory, allowing it to run far more software than it could store in its RAM alone. With too little RAM, the kernel deals with page faults using a fiendishly complex set of manoeuvres. This takes time and slows the computer significantly. Sometimes you can even hear the large amount of disk activity it causes. This thrashing is a sign that the system needs more (usually inexpensive) RAM rather than a costly new processor.

To help use RAM even more efficiently, Windows also uses a system of dynamic link libraries (DLLs). These are libraries of subroutines required by

several programs. Rather than every process containing the same code, they link to the relevant shared DLLs. To see any of this activity on a running system, however, you need to use something better than Task Manager.

USING PROCESS EXPLORER

Process Explorer is a replacement for Task Manager that displays far more information and provides more control over the running system. The program doesn't require installation as such. Just download it (see Useful Links for the URL), open the Zip file and drag and drop the procexp.exe file to a convenient place such as the desktop. Double-click the icon to run it.

The main screen lists all the processes currently known to the kernel. If you select one, the lower pane displays the list of DLLs it uses, which can be extensive. If you can't see the lower pane, press Ctrl-L to toggle it on and off. If the lower panel is showing but does not seem to list DLLs, press Ctrl-D.

Scroll down the process list in the top pane. You'll see it's divided into trees of processes. Some are owned by the System process, while others are owned by Explorer. In Windows XP, all system services are children of the System process, beginning with the Windows NT Session Manager. This shows that Windows XP really is built on the old Windows NT family of technologies.

You can sort the list by any of the columns. Click on a column heading to sort by how much processor power each process is using (CPU), how much memory it uses (Working Set) and the name of the program running it (Command Line). There are plenty of columns you can add to the display by choosing Select Columns from the View menu. You can also save a particular mix of columns using Save Column Set... on the same menu. This means you can quickly load a set of columns for a specific job, which is useful if you have a busy computer to manage and need to find out what's happening quickly. By selecting the relevant options on the Options menu, you can also change the colours and fonts used.

INTRODUCTION

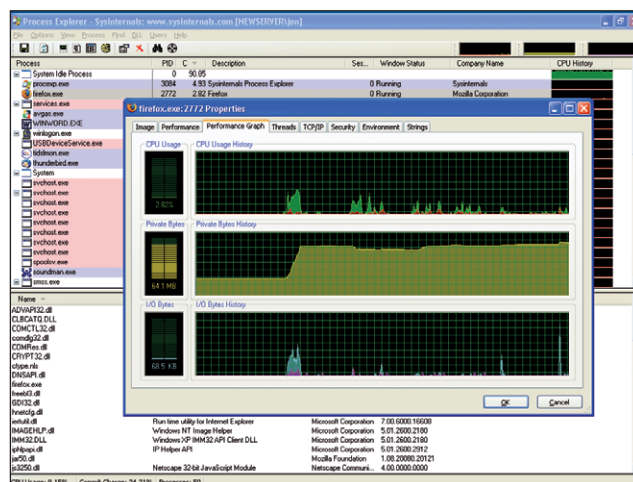
When your computer suddenly becomes sluggish, churning away at the hard disk and taking ages to switch between programs, you may well wonder what's going on behind the scenes. In fact, the safety of your files may depend on your knowing what tasks your PC is performing in the background.

But how do you tell if those strangely named processes listed by Task Manager are essential, uselessly consuming resources or, worse, malicious? Our guide will show you how to determine if they should be kept or killed.

Jon Thompson
IT Correspondent



contributors@computershopper.co.uk



▲ Double-click a process to get more detail about it, including graphs of its resource usage. This is not available with the standard Task Manager

USEFUL LINKS

Process Explorer <http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>

Information about rogue Helpsvc process
<http://support.microsoft.com/?kbid=839017>

Advice on curing a corrupt profile <http://support.microsoft.com/?kbid=555021>

A full list of all processes in a running Windows XP system
www.processlibrary.com

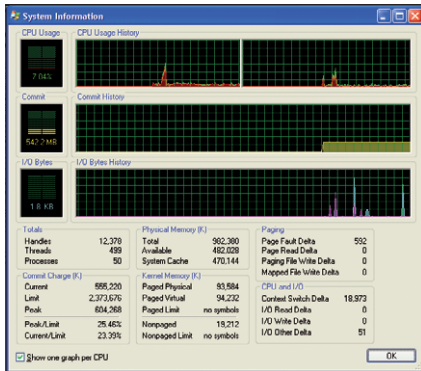
If you sort by a column with fast changing figures, the display might change too fast for you to make sense of it. Instead of sorting by processor, which changes all the time, try sorting by Window Status. This will show which processes are actually running.

TASK MANAGER REPLACEMENT

The Options menu contains an entry called Replace Task Manager. When selected, this runs Process Explorer instead of Task Manager so that when you press Ctrl-Shift-Esc you'll run Process Explorer. To ensure you don't run more than one instance of Process Explorer, also select the Allow Only One Instance option. To change back, select Restore Task Manager.

Hit Ctrl-I in Process Explorer and it will show you a similar Performance window to the one you usually get with Task Manager. This version carries more information about virtual memory and paging activity than the original. For instance, double-click on a running process and you'll bring up a window with eight tabs running across the top. Click the Performance tab to see how much virtual memory the application is using. The Performance Graph tab will show the processor, memory and data input/output, including network activity.

The TCP/IP tab can also be revealing. It shows the addresses of any remote servers with which



▲ Process Manager's System Information window contains useful memory data

the process is in contact. If you inspect the activities of a web browser, this tab shows the addresses of all the secondary websites to which you have connected. You might be surprised by the results, as many of these sites will be unknown to you.

You are connected to them
because the site you visit also

displays content from these third parties, perhaps as adverts, cookies and possibly even malware if the site has been compromised.

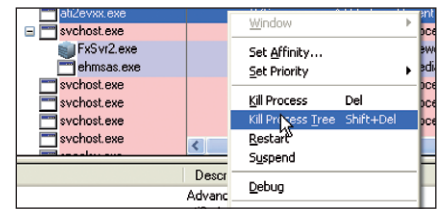
If you suspect the process in question has been spiked with malware you can verify its image signature, which will have changed if the program's code has been altered. Select the Image tab and press the Verify button. This will cause Process Explorer to calculate the program's checksum and contact sites that hold the correct image signature. If the image is correct then the status next to its icon will change to Verified. If you are suspicious of a process, this should be the first thing you do.

IDENTIFYING MALICIOUS PROCESSES

So what if your machine suddenly becomes sluggish, or the disk won't stop thrashing or Process Explorer finds an unknown process taking up all the processor time – is it malicious code? Here's how to discover what's going on.

A sudden thrashing problem may not be to do with malware at all, but could be a fault in the memory hardware. First, display the system information with Ctrl-I. You probably know what the total amount of physical memory should be – it's the amount displayed when the PC first boots. If Process Explorer reports a lower-than-expected figure, you have a problem. It may be a badly seated memory module, but if the problem persists it's time to replace your RAM chip. If the total amount of RAM is correct but the amount available is low, you probably need more RAM.

If you're suspicious of an unknown process, you need to know quickly if it's malicious or benign. Maybe it's taking up lots of processor or memory, or contacting unknown sites. Right-click on the process and select Search Online. This opens your web browser and interrogates Google. If the process is malicious, you'll soon find out by clicking on a few of the search



▲ Process Explorer offers a few process shutdown options to solve problems quicker than rebooting

results. In many cases, users have already found the same process and problem and can advise on a fix or point you to help provided by Microsoft.

Sometimes the advice you'll find on Google may tell you to kill a process. Process Explorer can do this for you. Right-click on the process in question and select Kill Process. By default, you'll be asked to confirm your wishes. If the process is controlling other (child) processes then select the Kill Process Tree option to shut down the whole family in an orderly fashion. An alternative is to try to restart the program. With Explorer, which occasionally crashes when you launch an application, experience shows that restarting it is better than a lengthy system reboot.

In some cases a heavy number-crunching job, such as encoding a movie in Windows Movie Maker, can mean that a program takes more of your computer's processor time than you'd like. If you have other things to do then this can be annoying, so you can also set the priority of a process by right-clicking it and selecting Set Priority. The movie encoding will continue but at a slower pace, enabling you to use your other applications without an unacceptably sluggish performance.

Occasionally processes do go wrong, but on a well-protected system you're more likely to encounter problems due to resource shortages and programming errors than malicious code. Applications such as Process Explorer put you in a good position to tell the difference and take the best steps to get your PC back up and running smoothly and quickly. **CS**

Next month

MASTER MEDIA STREAMING

Streaming media can be a challenge. We show you how to avoid the pitfalls

Time bandits Common system roguers

We occasionally see posts on technical support forums from worried users who have found that the System Idle Process is taking loads of processor time for itself. If this happens to you, don't worry: it's supposed to. A version of this process exists in all operating systems and literally does nothing. Its priority is so low that it can get processor time only when no other process needs it. By doing so, it gives a good measure of free processor capacity.

Some processes have a reputation for going wrong at a higher priority. One such culprit is Helpsvc, the Microsoft Help Centre Service. You'll only encounter this problem if you have Automatic Updates turned on. On an idle machine, this process can suddenly

take 100 per cent of the processor time. The initial cure is to kill the process (you don't have to reboot). Microsoft also recommends installing the latest service pack.

Sometimes, just right-clicking on a file will cause processor usage to shoot up to 100 per cent. This is to do with the `Csrss.exe` process and is caused by subtle corruption in your profile. Microsoft provides detailed instructions about how to correct a corrupt profile. See 'Useful Links' above for details.

If you're still using a software modem for making dial-up internet connections, you may find it's taking more processor time than is customary. Upgrade to the latest modem drivers or, if none is available, to a hardware modem – or opt for broadband.

Sometimes a process, especially an older application, will take increasingly large amounts of memory. You can see this happening by double-clicking on it in Process Explorer and opening its Performance Graph tab. This problem is caused by memory leakage, whereby the program allocates space for data and doesn't free it up again when it's done, before allocating more. Older versions of Microsoft Word suffer from this problem. The safest solution is a reboot.

Finally, if you don't recognise a process, you can always right-click on it in Process Explorer and identify it with the Search Online option. If it's malicious then you'll soon know, and will usually be able to find instructions on how to deal with it.